## Learning ElasticSearch 5.0

**Section 1: Getting Started with ElasticSearch**

**1.1 The Course Overview**

To get a feel for the course we do an end-to-end overview of what will be covered.

* Start by walking through the areas covered in the introductory section of the course
* Look at how to get started with the process of learning ElasticSearch
* Dive deeper into ElasticSearch's concepts and related technologies

**1.2 What Is ElasticSearch?**

Gaining a holistic view of a new technology is the first necessary step to learning how it works. ElasticSearch is introduced with accompanying use cases.

* Provide an introduction to ElasticSearch
* Highlight some key features of ElasticSearch
* Give example use cases

**1.3 Installing ElasticSearch**

Setting up a new technology is often a challenging affair. By walking through the simple process of installing ElasticSearch, developers can quickly move along the learning process.

* Install ElasticSearch
* Start up ElasticSearch cluster and install Kibana, the tool for data visualization and cluster management
* View Kibana in browser

**1.4 Goal of ElasticSearch**

Before diving into any new technology, it is all too important to understand what the subject technology was designed for and the best use cases. Peering into the objectives of ElasticSearch solves this.

* Highlight the primary goals of ElasticSearch
* Break down what it means to be Near Real-Time (NRT)
* Look at other ElasticSearch objectives

**1.5 What's New in Version 5.0?**

Version 5.0 of ElasticSearch has some key changes. Highlighting these changes help developers to get a better understanding of what's new.

* Identify noted changes in version 5.0
* Cover the new ElasticSearch application stack
* Look at lower level changes in ElasticSearch 5.0

**1.6 Why Use ElasticSearch?**

As is the case with any new technology, developers seek compelling use cases for implementing ElasticSearch. ElasticSearch answers the call by being a fairly straight forward, developer friendly analytics engine.

* Look at the developer friendly nature of ElasticSearch
* Show why ElasticSearch is great for search and analytics
* Give other compelling reasons to implement ElasticSearch

**Section 2: Dichotomy of ElasticSearch**

**2.1 What Is an Index?**

The indices are easily the cornerstone of ElasticSearch. As such, understanding indices and how they work is key.

* Define an index
* Define shards relative to an index
* Walk through the process of index creation

**2.2 Documents in ElasticSearch**

Documents hold data in ElasticSearch. Understanding the workings of documents put one on the path to better understanding ElasticSearch.

* Define a document
* Define type, which are key to document structure
* Gain understanding of document fields

**2.3 What Is a Cluster?**

The concept of a cluster can be broad and sometimes confusing. Understanding an ElasticSearch cluster is an important step in the learning process.

* Define an ElasticSearch cluster and associated nodes
* Explain partitioning of index into shards
* Discuss replicas and failovers

**2.4 Setting Shards and Replicas**

Distributed technology is extremely challenging to understand. Understanding how to set shards and replicas in ElasticSearch is therefore a necessary first step.

* Set number of shards
* Set number of replicas
* Confirm number of shards and replicas

**Section 3: Get Going with Documents and Indices**

**3.1 Adding and Deleting an Index**

Index and Mapping set the stage for data search and analysis. Knowledge of how each work is important for effective ElasticSearch usage.

* Add an index in ElasticSearch
* Setup mapping for documents
* Delete an index in ElasticSearch

**3.2 Adding and Deleting Documents**

Document addition and deletion in ElasticSearch controls the flow of data. The ability to add and delete documents in ElasticSearch is necessary.

* Add a document
* Delete a document
* Gain hands-on experience with adding and deleting documents

**3.3 Using Bulk API**

Since adding documents is among the most commonly performed tasks in ElasticSearch, there needs to be a way to add multiple documents simultaneously. The bulk API solves this problem.

* Add multiple documents in query body
* Add multiple documents from external file
* Gain hands-on experience with bulk API

**Section 4: Querying with RESTful API**

**4.1 Introduction to REST API**

Interfacing with technology from external systems can be challenging and often requires a high degree of expertise. The REST API in ElasticSearch solves this problem.

* Look at how the REST API makes interaction easy
* Gain an understanding of verbs / methods
* Walk through the dichotomy of a REST API request string

**4.2 Using REST API to Search**

Using REST API requires knowledge of how to run desired queries. Hands-on experience makes this possible.

* Use count API
* Use search API and match query
* Use pagination and term search

**4.3 Using REST API to Update**

One common point of confusion in REST technology is differentiating between PUT and POST. Gaining a clear understanding of PUT versus POST in updates is therefore key.

* Use PUT versus POST verbs
* Use REST Update API to update a document
* Get hands on experience with Update API via PUT and POST

**Section 5: Power Your Searches with DSL**

**5.1 Introduction to DSL**

Accessing the power of ElasticSearch necessitates understanding of its query language, DSL. A breakdown of DSL and how it works is essential.

* Define DSL (domain specific language) in ElasticSearch
* Look at the clauses that make up a DSL query
* Examine various types of queries

**5.2 Understanding DSL**

Moving beyond the basics in DSL can be challenging. Going beyond the basic to take a deeper look into DSL helps.

* Explain query context
* Look at relevance
* Explain filter context

**5.3 Term Queries and Boosting**

Understanding the type of queries required to gain optimal results is necessary in ElasticSearch. Knowledge of term queries and boosting helps to optimize query results.

* Define term query
* Explain boosting and how it effects query results
* Gain hands on experience with term queries

**5.4 Range Query**

Sometimes you will want to search a range of values. Range queries are the solution to this challenge.

* Explain range queries
* Discuss query parameters
* Get hands on experience with range queries

**5.5 Exist Query**

At times you will need to know when a given field exists. This is when you should turn to exist queries.

* Define exist query
* View example exist query
* Hands on experience in doing a search with the exist query

**5.6 Aggregation Based Analytics**

Generating analytics can be a challenging task. Built-in aggregation based analytics in ElasticSearch take the pain out of analytics.

* Explain metrics aggregation
* Explain bucket aggregations
* View examples of various types of metrics and bucket aggregations

**5.7 Aggregation Based Analytics**

The process of running aggregation based analytics in ElasticSearch can get confusing. Experience is the best teacher.

* Get average price
* Use geo bounds
* Perform analysis with extended\_stats and build date histogram

**Section 6: What ElasticSearch is NOT**

**6.1 Myths about ElasticSearch**

Not understanding the intended use of a technology can lead to bad implementations or even worse. It is imperative to understand what ElasticSearch is NOT designed for.

* Compare ElasticSearch to relational database systems
* Discuss when to use ElasticSearch
* Explain why ElasticSearch makes a better "in addition to…" system

**Section 7: Getting More with ElasticStack**

**7.1 What Is ElasticStack?**

ElasticSearch alone doesn't provide security, cluster management, log analysis and so on. Thus, ElasticStack was created.

* Define components of ElasticStack
* Discuss ElasticStack advantages
* Highlight importance of ElasticStack

**7.2 Kibana**

Data aggregation is the first of many steps in the analysis process. Kibana facilitates data visualization and acts as a cluster management interface.

* Define Kibana
* Walk through installation and setup process
* Gain hands on experience with installing and running Kibana

**7.3 Logstash**

Log analysis is an involved process that moves unstructured log data into the ElasticSearch cluster. Logstash was created for this very reason.

* Define Logstash
* Walk through the installation and setup process
* Gain hands on experience with installing and running Logstash

**7.4 X-Pack**

Prior to ElasticSearch 5.0, security, monitoring, alerting, reporting, graph and so on. were all separate components. Version 5.0 combined these to form X-Pack.

* Introduce X-Pack
* Walk through installation and setup process
* Gain hands on experience with installing and using X-Pack

**7.5 Beats**

The complexity of moving data from external systems to ElasticSearch presents many challenges. Beats was created to simplify the process of moving data into ElasticSearch.

* Define Beats
* Discuss different types of beats (File Beat, Metric Beat, Packet Beat and Winlog Beat)
* Walk through installation and setup process for File Beat

**Section 8: Apache Log Analysis**

**8.1 Preparing for Log Analysis**

Log analysis is a multi-step process that requires attention to detail. Clear understanding of the process is essential.

* Define Apache log analysis
* Explain the dichotomy of an Apache log message
* Walk through processes of building and testing logstash pipeline

**8.2 Running Log Analysis**

It's not enough to know the steps to the log analysis process. Practical experience is also necessary for true understanding.

* Gain hands on experience with preparing for log analysis
* Gain hands on experience with testing logstash pipeline and running full analysis
* View results of log analysis in Kibana

**Section 9: Advanced ElasticSearch Queries**

**9.1 Sorting in ElasticSearch**

In the world of data management, sorting is an absolute must have feature. Learning to sort in ElasticSearch can greatly improve search results

* Discuss the whats and whys of sorting
* Explain how sorting is done in ElasticSearch
* Gain hands on experience with sorting in ElasticSearch

**9.2 Geo Searching**

The ability to query Geo data highly ranks in modern use cases. ElasticSearch simplifies the process of geo searching.

* Define geo searching
* Explain geo distance and geo distance range
* Explain geo sorting

**9.3 Getting into Synonyms**

User generated queries for text search can be filled with colloquialism, abbreviations etc. Synonyms in ElasticSearch aim to help minimize this challenge.

* Define synonyms in ElasticSearch
* Examine components of ElasticSearch synonyms: filter and analyzer
* Dive deeper into synonyms

**Section 10: ElasticSearch versus Apache Solr**

**10.1 Choosing between ElasticSearch and Apache Solr**

ElasticSearch isn't the only high-octane text search engine in existence. Understanding a competing technology helps to identify where ElasticSearch stands.

* Discuss Apache Solr
* Provide comparison along with ElasticSearch advantages and challenges
* Render final comments